

REMARKS

This responds to the Final Office Action mailed on October 22, 2008.

Claims 2-18 and 21-25 are amended, no claims are canceled or added; as a result, claims 2-25 are now pending in this application.

Claim Objections

Claims 12, 16, 21, and 23 were objected to for various informalities. The claims have been amended herein to correct the noted informalities. The Applicants, therefore, respectfully request withdrawal of the claim objections.

§112 Rejection of the Claims

Claims 2-25 were rejected under 35 U.S.C. § 112, first paragraph, as lacking adequate description or enablement. The Office Action asserts on page 3 that, "the application as originally filed does not appear to discuss any program logic that installs on the playback device. While there may be an upgrade to software, firmware, or the like included with the content, such upgrade being performed if the proper conditions exist (such as authentication of the device and content), there does not appear to be any basis for "program logic installing on the playback device" as recited in claim 1."

The Applicants respectfully submit that the originally filed specification includes numerous portions of disclosure that describe and fully enable various aspects of program logic being loaded from user-accessible media (e.g., a disc) and executed from the playback device. A few of these portions of disclosure from the originally filed specification are set forth below.

In one exemplary embodiment, the player would have a user-accessible media input (consisting of a mechanized tray for one or more discs), which loads the media to a spindle where it is rotated and read using a laser. The data read from the media are brought to a microprocessor-based circuit, which analyzes the disc encoding to determine the capacity of the disc, formatting type, and security method. If the disc is a legacy (low resolution) DVD using the legacy security scheme (CSS), then the disc is played using methods known in the background art. If the disc is a high-density DVD using programmable security methods as disclosed herein, then program code (data processing instructions) for the content's security policies are loaded from the disc and executed by the player. Players can optionally also support low-density DVDs using the improved security, as well as high-density DVDs using legacy protection methods (although using a widely-broken security scheme for new content generally provides little

benefit). The quality of the output from the DVD player can be controlled by the content. (Present specification, pg. 33, lines 3-15, emphasis added).

...

In addition to interpreting player-independent, sandboxed code, the player may also allow the content to submit native code for execution and/or storage. Prior to accepting software or logic that may have access to keys or other privileged resources, the player validates the code. (Present specification, pg. 37, lines 14-16, emphasis added).

...

Successfully-validated native code may be stored in volatile memory for execution by the currently-loaded content, or it may be stored in the player's nonvolatile memory where it can be available to other titles. For example, to avoid possible negative effects on other titles, a patch to correct a cosmetic quirk in the player or to provide a performance optimization might be stored in volatile memory for use only by the currently-loaded title. In contrast, an upgrade to correct a security vulnerability would typically be stored permanently in the player's nonvolatile memory. Native code is normally specific to a single player platform or player application, making it less portable than interpreted code. Its advantage is that it can be used if needs arise that cannot be addressed using interpreted code. For example, native code can be employed by content as a way to distinguish between legitimate players and unauthorized emulators or "clones", avoiding the need to revoke every potentially-affected device each time attackers find a major security vulnerability in a product's design. (Present specification, pg. 37, lines 19-31, emphasis added).

...

In an exemplary embodiment of content employing native code, the media includes an initial boot portion consisting of interpreted code which, when interpreted, loads additional interpretable code. The content code (e.g., the code loaded by the boot portion) would then issue procedure calls to the player and analyze the results to determine information about the playback environment, including the player type. (Present specification, pg. 38, lines 13-17, emphasis added).

...

The native code can also be configured to perform an identifiable operation (such as a cryptographic computation that can be integrated with content decryption processes) so that content code can be assured that the native code was actually executed by the player. (Present specification, pg. 39, lines 7-10, emphasis added).

...

As described previously, a player device can provide content with nonvolatile (NV) storage capabilities for use by the content. (Present specification, pg. 41, lines 25-26, emphasis added).

Such disclosures, in combination with the remaining portions of the originally filed specification and figures, fully support and enable the, "program logic configured for installation on the playback device" as included in claim 2 and others of the pending claims.

Claim 2 has been amended herein to include, "the program logic further configured for cryptographically authenticating the revocations list." This language is also described and fully enabled in the originally filed specification in at the least the portions set forth below.

Media revocation checking can also be performed by code in the player's ROM. (Present specification, pg. 52, lines 28-29, emphasis added).

...
Revocation-related data fields may be cryptographically authenticated. (Present specification, pg. 53, lines 8-9, emphasis added).

Such disclosures, in combination with the remaining portions of the originally filed specification and figures, fully support and enable the, "the program logic further configured for cryptographically authenticating the revocations list" as included in claim 2 and others of the pending claims.

The Applicants, therefore, respectfully request withdrawal of the § 112, first paragraph claim rejections.

§103 Rejection of the Claims

Claims 2-13, 15-16, and 19-25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Asano (U.S. 6,999,587) in view of Benaloh (U.S. 7,065,216), Nonaka (U.S. Publication No. 2002/0035492), and Kyle (U.S. 6,141,681).

Claim 14 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Asano in view of Benaloh, Nonaka, and Kyle, further in view of Sugahra (EP 0 668 695 A2).

Claim 17 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Asano in view of Benaloh, Nonaka, and Kyle, further in view of Foote (U.S. 6,164,853).

Claim 18 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Asano in view of Banaloh, Nonaka, and Kyle, further in view of Ford ("Advanced Encryption Standard (AES) Questions and Answers," 10/2/2000, pp. 1-5, obtained from http://www.nist.gov/public_affairs/releases/aesq&a.htm).

The Applicants respectfully submit that the Office Action did not make out a *prima facie*

case of obviousness for at least the following reasons. Even if combined, the cited references fail to teach or suggest all of the claimed elements of Applicants' claimed embodiments. Further, there is no suggestion to combine the teachings of the numerous cited references, except from improperly using the Applicants' claimed embodiments as a template through hindsight reconstruction of the Applicants' claims.

In examining claims under 35 U.S.C. § 103(a), it is necessary for the Examiner to establish a proper prima facie case of obviousness before rejecting a claim as required by the Board of Patent Appeals and Interferences (BPAI). Such a rejection cannot be made if there is no evidence or suggestion in a cited reference of a claimed configuration. *Ex Parte Katoh et al.*, Appeal 20071460, Decided May 29, 2007. Further, it is improper to reject a claim when there is no suggestion to combine the teachings of the cited references, except from using the Applicants' invention as a template through hindsight reconstruction of the Applicants' claims. *Ex Parte Crawford et al.*, Appeal 20062429, Decided May 30, 2007. Moreover, a patent composed of several elements is not proved obvious merely by demonstrating that each element was, independently, known in the prior art *KSR Int'l v. Teleflex Inc.*, 127 S. Ct. 1727 (2007). See also M.P.E.P. § 2142. "[R]jections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." (See *In re Kahn*, 441 F. 3d 977, 988 (CA Fed. 2006) cited with approval in *KSR Int'l v. Teleflex Inc.*, 127 S. Ct. 1727, 1740-41 (2007)).

Moreover, the recent U.S. Supreme Court decision of *KSR v. Teleflex* provides a tripartite test to evaluate obviousness. "A rationale to support a conclusion that a claim would have been obvious is that ***all the claimed elements were known*** in the prior art and one skilled in the art could have combined the elements as claimed by known methods ***with no change in their respective functions***, and ***the combination would have yielded nothing more than predictable results*** to one of ordinary skill in the art." (See *KSR International Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 82 U.S.P.Q.2d 1385 (2007)). Emphasis added.)

Asano describes an information recording medium provided with: a user data recording part which records user data; a random-pattern-information recording part which records random pattern information from a random physical phenomenon; and an authentication data recording part which records, as authentication data, medium identification information created on the basis of the random pattern information detected from the random-pattern-information recording

part and a digital signature for each manufacturer with respect to the medium identification information.

In the Office Action, it is alleged that Asano discloses a digital optical medium containing a revocations list.

... the revocation list can be recorded in the authentication data recording part 5 of the optical disk 1. In the authentication data recording part 5 of the optical disk 1, the latest revocation list provided from the trusted center is recorded. (Asano, col. 8, lines 14-18).

However, the 'revocation list' described in Asano is not the same revocation list as presently claimed. In particular, Asano describes the use of its 'revocation list' as follows.

It is verified that the identification information ID of the manufacturer contained in the certificate (Cert) data is not in the revocation list stored in the nonvolatile memory (step S16). (Asano, col. 9, lines 53-56).

Thus, the data contained in the Asano revocation list is the ID of manufacturers determined to have committed a fraud (see Asano, col. 8, lines 19-24). The Asano 'revocation list' does not identify, "at least one revoked storage medium" as currently claimed. The Asano 'revocation list' is described as merely including the identification information ID of manufacturers. Thus, Asano does not describe or suggest this element of the claims as presently presented.

As correctly admitted in the Office Action, Asano does not disclose or suggest other elements of the pending claims (e.g., amended claim 2). Specifically, Asano is admitted as failing to disclose:

... that the list contains identifiers of revoked media, program logic for an interpreter of a Turing complete language, the program logic adapted for execution on a playback device in order to play the audiovisual content, the program logic installing on the playback device and cryptographically protecting on the playback device the revocations list, a plurality of versions of a plurality of portions of the digital audiovisual content where the versions for each portion may be distinguished from each other in pirated recordings of the audiovisual content; the versions are encrypted with different keys, such that each of the authorized playback devices is capable of deciphering at least one, but not all, of the versions for each of the portions; and the combination of the portions decipherable by a given player may be used to identify the player. (Office Action, pg. 7).

Therefore, Asano fails to describe or suggest significant portions of the embodiments as claimed.

Benaloh describes methods and systems that enable protection of digital content, such as movies and the like, by making pirated copies traceable back to a unique decryption key that was utilized to decrypt the originally encrypted content. Various embodiments can intrinsically link any unauthorized copies back to a unique cryptographic key or key collection that was used when the genuine copy was reproduced.

However, Benaloh does not describe or suggest a system wherein program logic for an interpreter configured for installation on the playback device is configured to provide a correct set of decryption keys for decrypting each of a plurality of versions of portions of the content. Unlike the presently claimed embodiments, Benaloh describes a system wherein, "[t]he DVD player 128 operates as an application program running on the operating system 126, and utilizes the operating system to access the DVD drive 106." The presently claimed embodiments do not operate as an application program and Benaloh does not describe the use of program logic for an interpreter configured for installation on the playback device and configured to provide a correct set of decryption keys. Therefore, Benaloh fails to describe or suggest elements of the embodiments as claimed.

Nonaka describes a data distribution system and method performing various processing such as suitable distribution of data, control of copying, conversion of signals, charging, and distribution of profits, comprising a reproducing apparatus for reproducing content data to be distributed from a mounted recording medium, a recording apparatus for recording reproduced content data on a mounted recording medium, an examining means for examining types of content data recorded on the recording medium, the recording medium mounted in the reproducing apparatus, the reproducing apparatus, a recording medium mounted in the recording apparatus and the recording apparatus, and a controlling means for controlling a transfer of the content data from the recording medium mounted in the reproducing apparatus to the recording medium mounted in the recording apparatus based on results of the examination.

Nonaka is offered in the Office Action as allegedly describing identifiers of revoked media and cryptographically protecting the revocations list on the playback device (Office Action, pg. 8). However, Nonaka describes a data distribution system, not a playback system. Nonaka does not describe program logic configured for installation on a playback device.

Nonaka does not describe the storage of versions of content or cryptographic keys on a playback device. Nonaka does not describe storage or use of a revocation list on a playback device. As such, Nonaka offers no motivation for being combined with the other cited references and no clue as to how such a combination could be implemented in the manner presently claimed. Therefore, Nonaka fails to render obvious the embodiments as claimed.

Kyle describes a data transfer system including a first computer which is operative to generate a data package having a data portion and an instruction portion. A second computer receives the data package through a transport media. The second computer is responsive to the data package to process the data portion in accordance with the instruction portion.

Kyle is offered in the Office Action as allegedly describing program logic for an interpreter as claimed. However, Kyle relates to data communication between computers and to transferring a data package including an instruction portion and a data portion wherein a receiving computer uses the instruction portion to process the data portion. Basically, Kyle describes a system for downloading executable code. Kyle does not describe the storage of versions of content or cryptographic keys on a playback device. Kyle does not describe using decryption keys for decrypting content on a playback device. Kyle does not describe storage or use of a revocation list on a playback device. As similar to Nonaka, Kyle offers no motivation for being combined with the other cited references and no clue as to how such a combination could be implemented in the manner presently claimed. Therefore, Kyle also fails to render obvious the embodiments as claimed.

Each of the pending claims includes elements distinguished from the cited referenced as explained above. Sugahra, Foote, and Ford also fail to describe or suggest significant portions of the embodiments as claimed. Further, these references offer no motivation for being combined with the other cited references and no teaching as to how such a combination could be implemented in the manner presently claimed. Such a combination of references can only come from improperly using the Applicants' claimed embodiments as a template through hindsight reconstruction of the Applicants' claims. Combinations of this type are clearly proscribed under applicable law. Therefore, Asano, Benaloh, Nonaka, Kyle, Sugahra, Foote, and Ford fail to render obvious the embodiments as presently claimed.

The Applicants, therefore, respectfully request withdrawal of the §103(a) rejections.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's representative at (408) 562-8496 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 13-0762.

Respectfully submitted,

MACROVISION SOLUTIONS CORP.

Dated: February 13, 2009

/Andy Pho/

Andy T. Pho

Reg. No. 48,862

MACROVISION SOLUTIONS CORP.

2830 De La Cruz Blvd.

Santa Clara, CA 95050

Phone: (408) 562 8496

Fax: (408) 567 1800